Google Updates from Threat Analysis Group (TAG)

THREAT ANALYSIS GROUP

Disrupting the Glupteba operation

Dec 07, 2021 · 3 min read

S **Shane Huntley**
Director, Threat Analysis Group

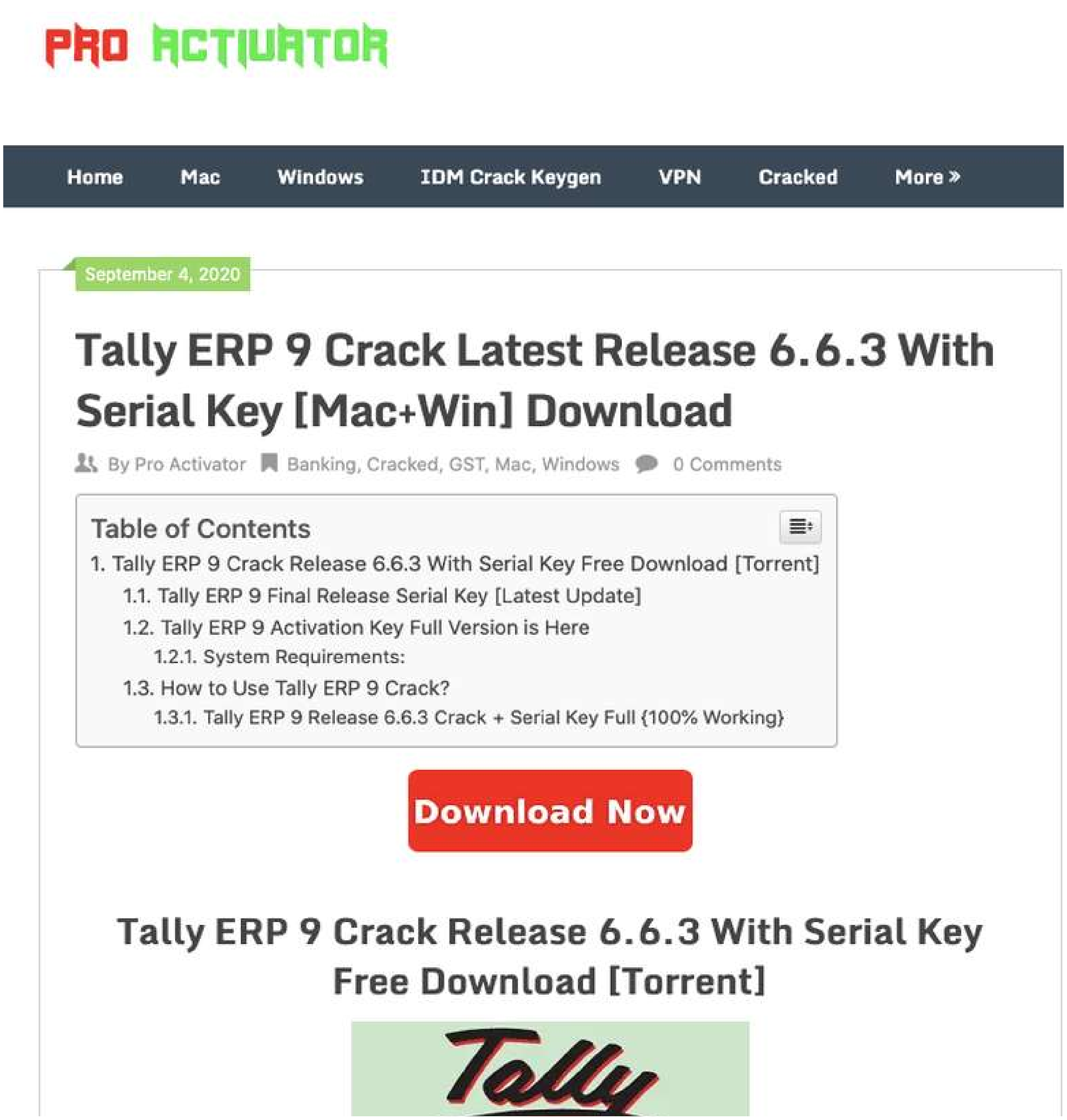
L **Luca Nagy**
Threat Analysis Group

Google TAG actively monitors threat actors and the evolution of their tactics and techniques. We use our research to continuously improve the safety and security of our products and share this intelligence with the community to benefit the internet as a whole.

As announced today, Google has taken action to disrupt the operations of Glupteba, a multi-component botnet targeting Windows computers. We believe this action will have a significant impact on Glupteba's operations. However, the operators of Glupteba are likely to attempt to regain control of the botnet using a backup command and control mechanism that uses data encoded on the Bitcoin blockchain.

Glupteba is known to steal user credentials and cookies, mine cryptocurrencies on infected hosts, deploy and operate proxy components targeting Windows systems and IoT devices. TAG has observed the botnet targeting victims worldwide, including the US, India, Brazil and Southeast Asia.

The Glupteba malware family is primarily distributed through pay per install (PPI) networks and via traffic purchased from traffic distribution systems (TDS). For a period of time, we observed thousands of instances of malicious Glupteba downloads per day. The following image shows a webpage mimicking a software crack download which delivers a variant of Glupteba to users instead of the promised software.



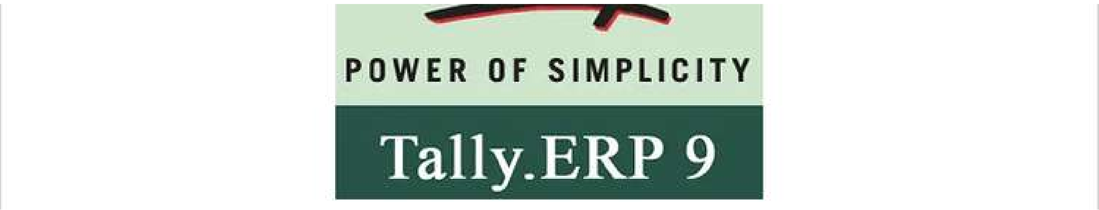
Tally ERP 9 Crack Latest Release 6.6.3 With Serial Key [Mac+Win] Download

By Pro Activator Banking, Cracked, GST, Mac, Windows 0 Comments

Table of Contents

1. Tally ERP 9 Crack Release 6.6.3 With Serial Key Free Download [Torrent]
   1.1. Tally ERP 9 Final Release Serial Key [Latest Update]
   1.2. Tally ERP 9 Activation Key Full Version is Here
      1.2.1. System Requirements:
   1.3. How to Use Tally ERP 9 Crack?
      1.3.1. Tally ERP 9 Release 6.6.3 Crack + Serial Key Full {100% Working}

Tally ERP 9 Crack Release 6.6.3 With Serial Key Free Download [Torrent]



Example cracked software download site distributing Glupteba

While analyzing Glupteba binaries, our team identified a few containing a git repository URL: “git.voltronwork.com”. This finding sparked an investigation that led us to identify, with high confidence, multiple online services offered by the individuals operating the Glupteba botnet. These services include selling access to virtual machines loaded with stolen credentials (dont[.]farm), proxy access (awmproxy), and selling credit card numbers (extracard) to be used for other malicious activities such as serving malicious ads and payment fraud on Google Ads.

BitcoinRevolution
EN
BITCOIN REVOLUTION
Access the Bitcoin Revolution App to Trade Digital Financial Assets Become Part of the Bitcoin Revolution Official Website Today

Example of a cryptocurrency scam uploaded to Google Ads by Glupteba services

This past year, TAG has been collaborating with Google's CyberCrime Investigation Group to disrupt Glupteba activity involving Google services. We've terminated around 63M Google Docs observed to have distributed Glupteba, 1,183 Google Accounts, 908 Cloud Projects, and 870 Google Ads accounts associated with their distribution. Furthermore, 3.5M users were warned before downloading a malicious file through Google Safe Browsing warnings.

In the last few days, our team partnered with Internet infrastructure providers and hosting providers, including Cloudflare, to disrupt Glupteba's operation by taking down servers and placing warning interstitial pages in front of the malicious domain names. During this time, an additional 130 Google accounts associated with this operation were terminated.

Parallel to the analysis, tracking, and technical disruption of this botnet, Google has filed a lawsuit against two individuals believed to be located in Russia for operating the Glupteba Botnet and its various criminal schemes. Google is alleging violations under the Racketeer Influenced and Corrupt Organizations Act (RICO), the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, the Lanham Act, and tortious interference of business relationships, and unjust enrichment.

While these actions may not completely stop Glupteba, TAG estimates that combined efforts will materially affect the actor's ability to conduct future operations.

Glupteba's C2 Backup Mechanism

The command and control (C2) communication for this botnet uses HTTPS to communicate commands and binary updates between the control servers and infected systems. To add resilience to their infrastructure, the operators have also implemented a backup mechanism using the Bitcoin blockchain. In the event that the main C2 servers do not respond, the infected systems can retrieve backup domains encrypted in the latest transaction from the following bitcoin wallet addresses:

'1CgPCp3E9399ZFodMnTSSvaf5TpGiym2N1' [1]

'15y7dskU5TqNHXRtu5wzBpXdY5mT4RZNC6' [2]

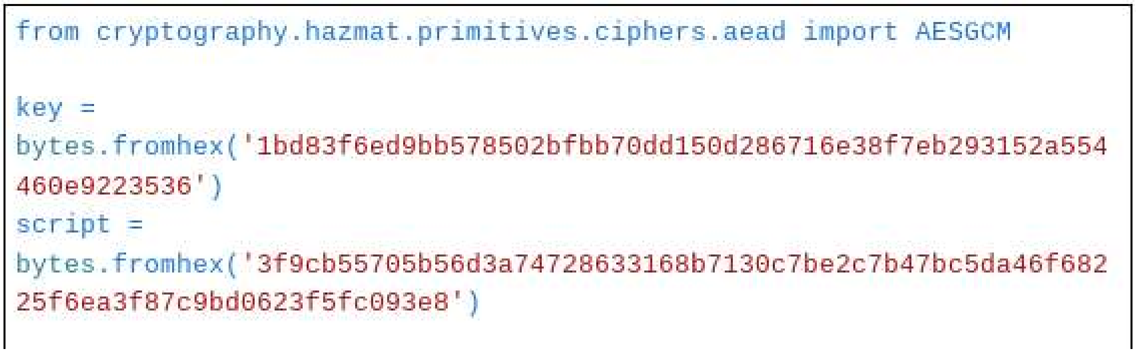
'1CUhaTe3AiP9Tdr4B6wedoe9vNsymLiD97' [3]

The following 32 byte AES keys for decryption are hard coded in the binaries:

'd8727a0e9da3e98b2e4e14ce5a6cf33ef26c6231562a3393ca465629d66503cf'

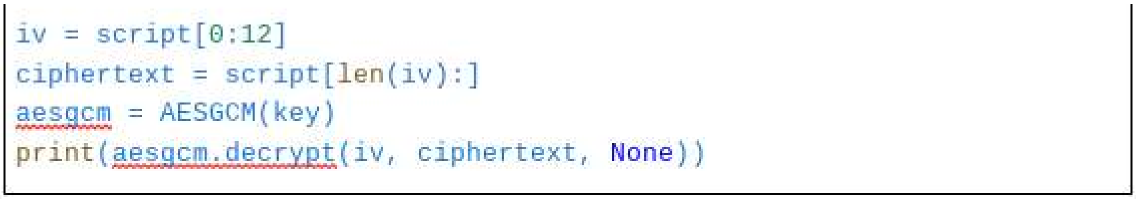
'1bd83f6ed9bb578502bfbb70dd150d286716e38f7eb293152a554460e9223536'

The blockchain transaction's OP_RETURN data can be decrypted using AES-256 GCM to provide a backup command and control domain name. The first 12 bytes of the OP_RETURN contains the IV, the last 16 bytes the GCM tag, while the middle section is the AES-256 GCM encrypted domain. Full details of Glupteba's network protocol can be found in this report from 2020, the following Python script illustrates how one can decrypt an encrypted domain name:



```
from cryptography.hazmat.primitives.ciphers.aead import AESGCM

key =
bytes.fromhex('1bd83f6ed9bb578502bfbb70dd150d286716e38f7eb293152a554
460e9223536')
script =
bytes.fromhex('3f9cb55705b56d3a74728633168b7130c7be2c7b47bc5da46f682
25f6ea3f87c9bd0623f5fc093e8')
```



```
iv = script[0:12]
ciphertext = script[len(iv):]
aesgcm = AESGCM(key)
print(aesgcm.decrypt(iv, ciphertext, None))
```

IOCs

Recent domains used for command and control:

nisdably[.]com

runmodes[.]com

yturu[.]com

retoti[.]com

trumops[.]com

evocterm[.]com

iceanedy[.]com

ninhaine[.]com

anuanage[.]info

Recent sha256 hashes of malware samples:

df84d3e83b4105f9178e518ca69e1a2ec3116d3223003857d892b8a6f64b05ba

eae4968682064af4ae6caa7fff78954755537a348dce77998e52434ccf9258a2

a2fd759ee5c470da57d8348985dc34348ccaff3a8b1f5fa4a87e549970eeb406

d8a54d4b9035c95b8178d25df0c8012cf0eedc118089001ac21b8803bb8311f4

c3f257224049584bd80a37c5c22994e2f6facace7f7fb5c848a86be03b578ee8

8632d2ac6e01b6e47f8168b8774a2c9b5fafaa2470d4e780f46b20422bc13047

03d2771d83c50cc5cdcbf530f81cffc918b71111b1492ccfdcefb355fb62e025

e673ce1112ee159960f1b7fed124c108b218d6e5aacbcb76f93d29d61bd820ed

8ef882a44344497ef5b784965b36272a27f8eabbcbcea90274518870b13007a0

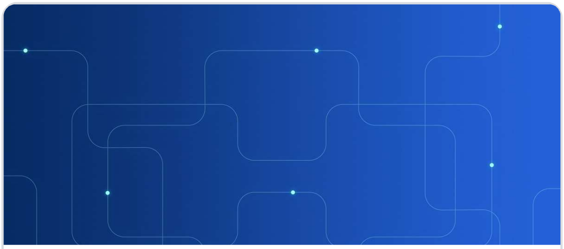
79616f9be5b583cefc8a48142f11ae8caf737be07306e196a83bb0c3537ccb3e

db84d13d7dbba245736c9a74fc41a64e6bd66a16c1b44055bd0447d2ae30b614

POSTED IN:

Threat Analysis Group

Related stories



THREAT ANALYSIS GROUP

New Iranian APT data extraction tool

THREAT ANALYSIS GROUP

TAG Bulletin: Q2 202

This bulletin includes coordina influence operation campaigns terminated on our platforms in 2022. It was last updated on Ju 2022.

Aug 23, 2022 →

Jul 29, 2022

○ ○ ○ ○ ○ ○

Google serves cookies to analyze traffic to this site. Information about your use of our site is shared with Google for that purpose. See details.

OK